

⑯ 公開特許公報 (A)

昭62-49595

⑮ Int.Cl.¹G 06 K 19/00
B 42 D 15/02
G 06 F 12/14

識別記号

庁内整理番号

⑯ 公開 昭和62年(1987)3月4日

6711-5B

7008-2C

B-7737-5B 審査請求 未請求 発明の数 1 (全5頁)

⑯ 発明の名称 I Cカードのメモリ管理方法

⑯ 特願 昭60-190821

⑯ 出願 昭60(1985)8月29日

⑯ 発明者 原田 雅之 横浜市港北区綱島東4丁目3番1号 松下通信工業株式会社内

⑯ 発明者 山口 哲夫 横浜市港北区綱島東4丁目3番1号 松下通信工業株式会社内

⑯ 発明者 今 敏則 横浜市港北区綱島東4丁目3番1号 松下通信工業株式会社内

⑯ 発明者 井上 慎治 横浜市港北区綱島東4丁目3番1号 松下通信工業株式会社内

⑯ 出願人 松下電器産業株式会社 門真市大字門真1006番地

⑯ 代理人 弁理士 中尾 敏男 外1名

最終頁に続く

明細書

1. 発明の名称

I Cカードのメモリ管理方法

2. 特許請求の範囲

I Cカードのメモリエリアを複数のブロックに分割し、それぞれのブロックにはそれぞれ別個の読み出し不能なパスワードを対応させるようにしたI Cカードのメモリ管理方法。

3. 発明の詳細な説明

産業上の利用分野

本発明は、複数の情報について全く独立して秘密を保つためのI Cカードのメモリ管理方法に関する。

従来の技術

従来、I Cカードは、そのI Cカードが正当であることを証明したり、本人であることの確認をしたりするためのパスワードを1種類しか持っていないなかった。従ってパスワードが一致すれば、I Cカード内メモリのアクセス可能エリアはすべてアクセスすることができた。

第5図は、ハネウェルブル社のC P 8カードの構成をブロック図で表現したものである。1はC P 8カード全体、2はマイクロプロセッサ、3と4と5を総称してメモリエリアといい、3はシークレットエリア、4はコンフィデンシャルエリア、5はデータエリアである。C P 8カード1には機密保護機能としてこの3つのアクセスレベルを有しており、マイクロプロセッサ2の働きにより、

・シークレットエリアのデータ

カードの外部には決して転送されない。

・コンフィデンシャルエリアのデータ

カード及びカードの使用者の確認後、外部に転送可能である。

・データエリアのデータ

同一用途の端末によって自由に読み取り書き込みができる。

のようにメモリ内データが管理されている。C P 8カード1では、本発明で述べるところのパスワードは、シークレットエリア3に書き込まれ、こ

のパスワードは決して外部に転送されないので、読み出すことができない。外部制御部から、外部端子を通して、マイクロプロセッサ2にパスワードを送ると、マイクロプロセッサ2は、シークレットエリア3内のパスワードと照合し、合致すれば、外部制御部からの、コンフィデンシャルエリア4へのアクセスを許す。このようにパスワードにより、カード使用者の本人確認及びカードの正当性のチェックが行われると、このコンフィデンシャルエリア4のデータをすべて、マイクロプロセッサ2を経由して外部に取り出すことができた。

発明が解決しようとする問題点

上記従来のICカードのメモリ管理方法では、パスワードが1種類であって、また、この1種類のパスワードが合致すると、メモリ内のアクセス可能なエリアのデータは、すべて読み出し可能であった。

従って、例えば複数の営利企業がその顧客サービスのために1枚のICカードを共用しようとする

る際に、それぞれの企業秘密事項をICカードメモリに書き込もうと思っても、その秘密事項は1つのパスワードでのチェックの合致だけですべて読みとることが可能になってしまい、他社の秘密事項が漏洩してしまうという問題があった。

現在の磁気カードシステムにおいては、各銀行、各クレジット会社、各流通サービス業者等がそれぞれ独自の磁気カードを発行しているので、顧客は複数の磁気カードを持ち運ばねばならないという不便があり、磁気カードより大容量のメモリ機能を有するICカードで、複数の磁気カード機能を統合化しようと考えても、従来のICカードのメモリ管理方法では各社の企業秘密が漏れてしまい、統合化できないという問題点があった。

本発明は、このような従来の問題を解決するものであり、複数の企業が、1枚のICカード内にそれぞれのデータを共存させても、企業秘密の漏洩を防ぐことができる優れたICカードのメモリ管理方法を提供することを目的とするものである。

問題点を解決するための手段

本発明は上記目的を達成するために、ICカードメモリエリアを複数個に分割し、それぞれにパスワードエリアとデータエリアを設けるように構成したものであり、それぞれのデータエリアにアクセスするには、それぞれのパスワードとの照合を行わねばならないとの制約を課したものである。

作用

したがって、本発明によれば、複数のデータエリアに対応してそれぞれのパスワードを有するので、複数の営利企業が、1枚のICカード内にデータを共存しようとするとき、それぞれ1社が1つのパスワードを用いることによってそれぞれのデータエリア内の情報をお互いに漏洩不能にすることができる。すなわち、顧客にとって、1枚のICカードさえ所有していれば、複数の競合する営利企業からでもそれぞれ別のサービスを受けることができ、企業側としても秘密の保守ができるという効果を有する。

もし、あるデータエリアは各企業とも共通に使いたいとするならば、使いたい企業には、そのデータエリアに対応するパスワードを公開しておけば良い。

実施例

第1図は本発明の一実施例の構成を示すものである。6はICカード全体、7はマイクロプロセッサ、8はメモリ、9は外部端子、10は外部制御部である。メモリ8は、マイクロプロセッサ7を介して外部端子9と接続している。外部制御部10からメモリ8へアクセスするためには、マイクロプロセッサ7を介しておこなう。

第2図は、第1図のメモリ構成をより詳細に示したものである。メモリサイズは2048バイト(2Kバイト)の例で説明する。最少の1まずは1バイトである。1桁を32バイトとし、0桁から63桁までに分け、それぞれ4桁づつを組み合わせて第0ブロックから第15ブロックまでを作る。それぞれのブロックの先頭桁の第0バイト目から第11バイト目までをパスワードエリアとし、残りをデータ

タエリアとする。このようにしてパスワードエリアとデータエリアを持ったブロックが16組構成できる。

次に上記実施例の動作について説明する。第3図は外部制御部10から本発明のICカード6に向っての、外部制御部10のフローチャート、第4図は、ICカード6内のマイクロプロセッサ7とメモリ8のフローチャートである。第3図と第4図にA、B、C……Gの記号を付したが、第3図のAと第4図のAと対応している。同様にBとB、CとCそれぞれの対応を示している。第3図において、外部制御部10は、まずICカード6に対してパスワードの登録を行う。パスワード登録可能かどうかをICカード6に対して問うと、ICカード6から返信が返ってくる。“OK”であれば、パスワードを送信し、ICカード6内のマイクロプロセッサ7の働きにより、メモリの空きブロックの1つのパスワードエリアにパスワードを登録する。続いてそのブロックのデータエリアには、データのリードライト（読み出し書き込み）が行

える。終了時には“END”電文をICカード6に対して送信する。Bの返信受信が“OK”でない場合には、ICカード6のブロックはすべてすでに使われてしまっていて新規にパスワードが登録できないことを示している。

次に、すでにパスワードを登録して、データエリアにデータが書き込んである場合の、データエリアへのアクセスの手順を説明する。第3図のメモリアクセスフローチャートにおいて、Fでパスワードを送信する。ICカード6内のマイクロプロセッサ7はメモリ8の各ブロックを調べ、同一のパスワードがすでに登録されているかどうか調べ、あれば“OK”を返し、そのブロックのデータエリアへのアクセスを許す。もし同一のパスワードがまだ登録されていなければ、“NG”を返して終了する。

第4図はICカード6内のフローチャートである。Aの初期電文受信にて、パスワードの新規登録を外部制御部10が要求しているのかどうかがわかる。パスワードの新規登録を要求されているの

であれば、メモリに空きブロックがあるかをICカード6内のマイクロプロセッサ7が調べ、空きブロックがあれば“OK”を送信し、続いてパスワードを受信し、その空きブロックにパスワードを新規登録し、そのブロックのデータエリアへのリードライトを許す。またAの初期電文受信にて、すでに登録済のパスワードのブロックへのアクセスを要求されているのであれば、Fでパスワードを受信し、該当するパスワードがあるかを、ICカード6内のマイクロプロセッサ7が調べ、同一パスワードがあれば、そのブロックのデータエリアへのアクセスを許す。同一パスワードがなければ、外部制御部10に対して“NG”を送信して終る。

第2図において、メモリサイズを、2Kバイトの場合で説明したが、メモリサイズが8Kバイトの例であれば、同様のブロックが64組構成できる。32Kバイトメモリであれば256組構成できる。

また、パスワードを12バイトの例で説明したが、

セキュリティ向上の要望に応じて、何バイトで構成しても構わない。

発明の効果

本発明は、上記実施例より明らかなように、ICカードのメモリを複数のブロックに分割し、それぞれにパスワードを設けて、ICカード内のマイクロプロセッサの制御の下に管理するようにしたので、それぞれのブロックは、それぞれ独立して秘密を保つことができる。このため、利害の反する複数の企業が、例えば、複数の銀行、クレジット会社、流通業者が、1枚のICカードを共用してサービスを提供することができるので、カード所有者たる顧客は、ただ1枚のICカードで複数の企業から別々のサービスを受けられる効果を有する。

4. 図面の簡単な説明

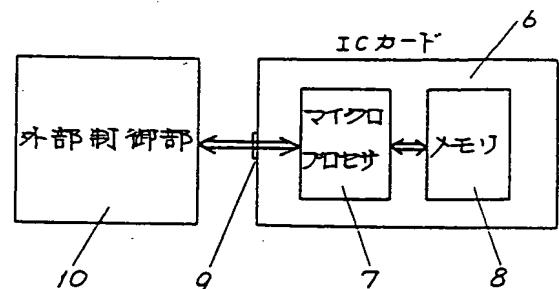
第1図は、本発明の一実施例におけるICカードと外部制御部のブロック図、第2図は、第1図におけるメモリ構成の詳細、第3図は、外部制御部から、本発明のICカードに向かっての外部制

御部のフロー・チャート、第4図は、本発明のICカード内のマイクロプロセッサとメモリのフロー・チャート、第5図は、従来のICカードの概略ブロック図である。

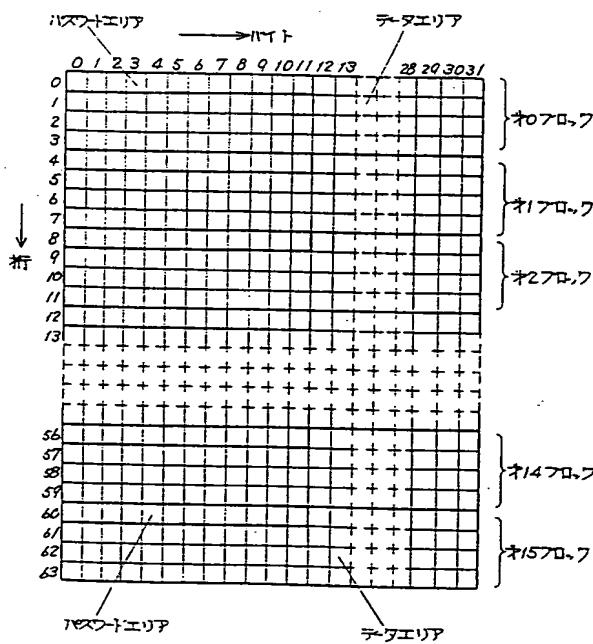
6……ICカード、7……マイクロプロセッサ、8……メモリ、9……外部端子、10……外部制御部。

代理人の氏名 弁理士 中尾敏男 ほか1名

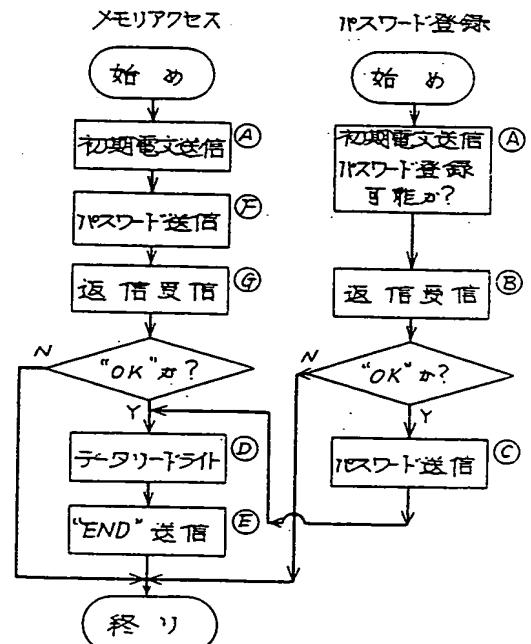
第1図



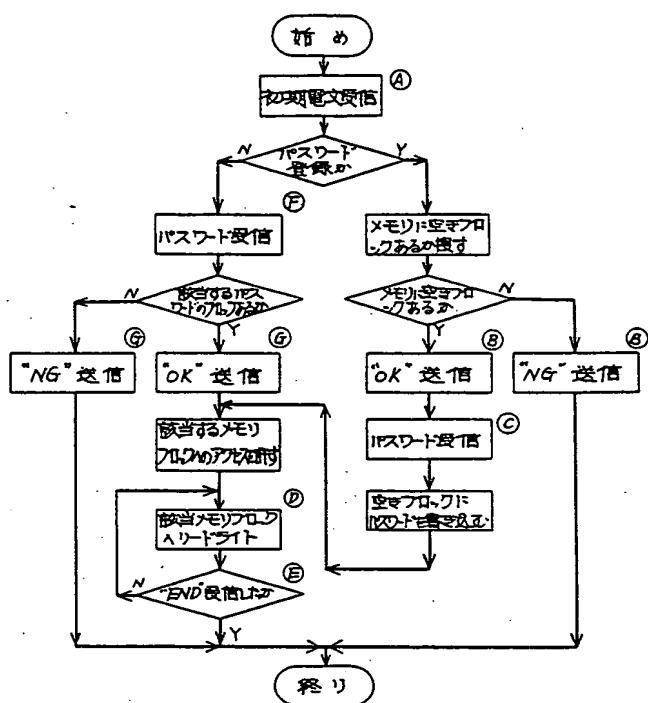
第2図



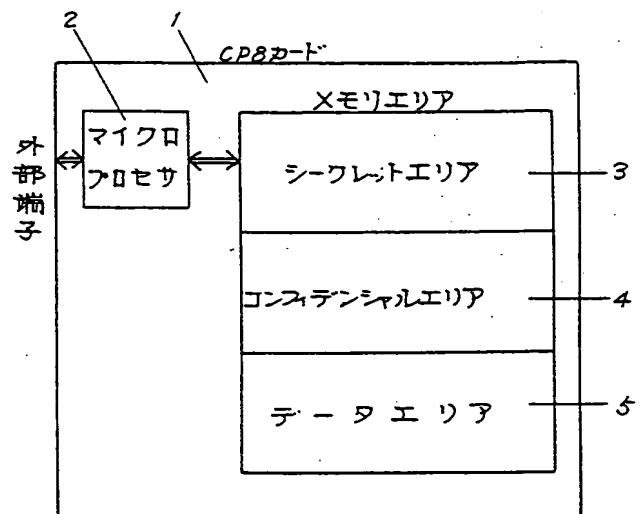
第3図



第 4 圖



第 5 図



第1頁の続き

⑦発明者 藤田 幹男 横浜市港北区綱島東4丁目3番1号 松下通信工業株式会社内